



National Infrastructure Protection Center

NIPC Daily Open Source Report

for 03 February 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports New York State announced on Thursday that it could not approve an emergency plan for the area around the Indian Point nuclear plant, asking the federal government to take the next step in the fierce battle over the two reactors in Westchester County. (See item [2](#))
- The U.S. Customs Service reports Commissioner Robert C. Bonner announced that the Customs Service will begin enforcing the 24-hour advance manifest regulation on Sunday, February 2. (See item [14](#))
- CNN reports the Red Cross' Blood Services Southern Region has asked hospitals in Georgia to hold some units of donated blood while the Red Cross investigates a problem with blood bags. (See item [19](#))
- The Washington Post reports that the newly formed Department of Homeland Security was immediately informed of the shuttle disaster and would take part in the investigation. (See item [22](#))
- Federal Computer Week reports the Institute for Information Infrastructure Protection has unveiled its 2003 Cyber Security Research and Development Agenda, which identifies critical areas that require significant research and development to help secure the nation's information infrastructure. (See item [29](#))
- Note from the Editor: The NIPC Daily Report is being distributed through a new list service and ISP. While we have reviewed the distribution process for errors, there will undoubtedly be some problems. Please contact deford@mitre.org with any problems.
- Note from the Editor: Both the PDF and Word versions of the daily are posted to the NIPC Web Site at <http://www.nipc.gov/dailyreports/dailyindex.htm>

NIPC Update Fast Jump

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 31, Platts Global Energy News* — **LNG vital to fill growing U.S. gas supply gap: CERA report. Huge growth in liquefied natural gas (LNG) imports will be required to fill a "looming natural gas supply gap" in the U.S., according to a new report by Cambridge Energy Research Associates (CERA). In fact, LNG -- which now makes up just 0.1% of the country's gas consumption -- could account for as much as 11% of domestic gas within seven years, CERA said.** "In all, natural gas demand is expected to increase by 14% by 2010, while US production will be 6% lower," according to Bob Ineson, CERA's director of North American natural gas. "As U.S. demand for gas increases, particularly for gas-fired electric power generation, LNG could supply as much as 11% of the total market demand by 2010." LNG volumes ultimately will have to soar to 9 Bcf/day (billion cubic feet) to match demand growth, CERA said. **CERA also looked at other "frontier resources" for U.S. gas supply. "Increased Rockies production will play an increasing role, as will Atlantic Canada and the deep-water Gulf," Zenker said. CERA also compared Alaskan gas and LNG and found that "LNG is well under way, whereas Alaska gas is more in a planning stage."** According to CERA Director Robert Esser, even with gas prices as high as \$5/Mcf (million cubic feet) this winter "drilling activity is lagging, and an expected increase in drilling activity that should start later this year is not likely to produce anything more than a modest increase in production by mid-decade. None of this will be enough to stem the long-term decline in North American natural gas production."
Source: <http://www.platts.com/stories/home2.html>
2. *January 31, New York Times* — **Albany says it can't certify Indian Point evacuation plan.** New York State said yesterday that it could not approve an emergency plan for the area around the Indian Point nuclear plant, asking the federal government to take the next step in the fierce battle over the two reactors in Westchester County. **Gov. George E. Pataki did not comment on the merits of the emergency plan, which has come under increasing attack since a consultant he hired reported this month that it was inadequate to protect the public from a release of radiation, especially a large release from a terrorist attack. But Mr. Pataki said in a statement that the report "has heightened our concerns about the adequacy of the emergency plans for these communities."** Today is the deadline for New York to issue its normally routine annual certification of the emergency plan, which the state drafts in consultation with federal and local officials and the plant owner. But the state told federal officials yesterday that it could not give that approval because the four counties surrounding the plant, concerned about safety, had refused to issue their own certifications. In effect, the governor sought to shift the focus to federal agencies, which will decide what happens next and will face pressure from opponents of Indian Point to close the plant, 35 miles north of Midtown Manhattan, in Buchanan. **In a letter to the Federal Emergency Management Agency**

(FEMA), the state said it simply could not give its annual certification to the plan because the four counties had refused to submit required "checklists." Those forms confirm that the counties have performed necessary training and drills and have completed various administrative functions. Pataki urged FEMA and the Nuclear Regulatory Commission, which requires a FEMA-approved plan as a condition of the plant's operating license, to heed the counties' concerns and "continue working with us to ensure that these plans will protect our residents in the event of a nuclear emergency." Although the Nuclear Regulatory Commission requires a FEMA-approved plan, it has never closed a plant over emergency planning problems; in fact, it has never closed a plant permanently against an owner's will. Even if it decides an evacuation plan is inadequate, the commission can give the plant owner a chance to show that the plan is adequate or that the owner can address the problems. The commission can also let the owner offer "other compelling reasons for continued operation," and Entergy has often pointed out that Indian Point contributes at least one-fifth of the electricity for New York City and its northern suburbs.

Source: <http://www.nytimes.com/2003/01/31/nyregion/31INDI.html>

3. *January 31, Daily News Bulletin* — **The Kavkasioni power transmission line, through which Russia delivers power to Georgia, has been damaged by an armed attack. The Georgian Fuel and Energy Ministry told Interfax that unidentified gunmen fired automatic weapons at electric insulators at the power transmission line in the Tsalendzhikha district in the early hours of Friday.** The amount of time necessary for repair work cannot yet be estimated, the ministry said. Due to the damage, Georgia has been deprived of about 350 megawatts of power, which has paralyzed the nation's entire power system. **At present, Georgia is receiving only about 120 megawatts of electricity from Armenia. Georgia itself is producing no more than 650 megawatts, the ministry said. This is the third time this winter the Kavkasioni power transmission line has been damaged.**

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3616356

4. *January 30, U.S. Department of Transportation, Office of Public Affairs* — **RSPA delivers on gas pipeline safety with integrity management.** A rule to improve the safety and reliability of natural gas pipelines has been proposed by the U.S. Department of Transportation's Research and Special Programs Administration (RSPA). **RSPA's Office of Pipeline Safety is the federal authority for the safety of the nation's 2.3 million miles of natural gas and hazardous liquid pipelines. The proposed rule is designed to identify the best methods for maintaining the structural soundness, or integrity, of pipelines.** "Pipeline safety is a top priority of RSPA, and we are delivering results," said Ellen G. Engleman, RSPA administrator. "Continuous improvement in pipeline integrity management is essential to ensuring public confidence in the safety and reliability of our nation's growing pipeline infrastructure." This proposed rulemaking incorporates the integrity management mandates of the Pipeline Safety Improvement Act, signed into law last Dec. 17. Under this rule, pipeline operators would face stringent requirements for testing and repair. They would have to comprehensively evaluate their pipelines and take measures to protect those segments where failure could impact populated areas. **RSPA has public responsibilities for safe, reliable and secure movement of hazardous materials to industry and consumers, by all transportation modes including the nation's pipelines; rapid response to emergencies by government agencies; training for transportation safety professionals; and applying science and technology to meet national transportation needs.** The Notice of Proposed Rule Making was published in the Federal

Register on Jan. 28, 2003 for a 60-day public comment period as Docket No. RSPA-00-7666; Notice 4.

Source: <http://www.dot.gov/affairs/rspa0203.htm>

5. *January 30, Reuters* — **PPL isolates radioactive gas release at Pennsylvania nuke plant. Pennsylvania energy giant PPL Corp. said it isolated a "higher-than-normal radioactive gas release" at its Susquehanna nuclear station in eastern Pennsylvania, according to a statement. At 8:32 p.m. Eastern time (1332 GMT) on Wednesday, PPL said the two-unit 2,200 megawatt plant entered the lowest of the four emergency classifications for nuclear power plants after monitors briefly indicated the gas release from the unit 1 turbine building vent. In less than an hour, the statement said monitor readings returned to normal and have remained there since.** Herbert Woodeshick, special assistant to the president for PPL Susquehanna, which operates the plant for PPL, said in the statement "the general public was not threatened and no action by the general public was required." Plant personnel investigating the situation determined that drain valves malfunctioned, allowing a small amount of radioactive gases to bypass the plant's off-gas system. The system is used to separate any gases from steam that has passed through the plant's turbine and treat those gases before they are released into the atmosphere. **PPL notified Luzerne and Columbia county emergency management agencies, the Pennsylvania Emergency Management Agency and the Nuclear Regulatory Commission of the incident.**

Source: http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3612379

[\[Return to top\]](#)

Chemical Sector

6. *January 31, Associated Press* — **Ignitable dust may have caused North Carolina blast.** Investigators developed a theory on what caused a deadly explosion at a medical supply plant even before they could douse a lingering rubber fire and go inside the twisted ruins. **Dust generated in the course of making rubber could have formed a combustible cloud that erupted at the West Pharmaceutical Services Inc. plant in Kinston, NC, the U.S. Chemical Safety and Hazard Investigation Board said Thursday.** The blast shot flames and debris high into the air and shook buildings miles away Wednesday afternoon. Of about 130 people inside the plant, three were killed and 15 remained hospitalized late Thursday, 10 of them in critical condition. **The factory, opened in 1975, employed 255 people making syringe plungers, intravenous equipment and rubber for medical equipment. The process of making the rubber, known as polyisoprene, produces "significant quantities of dust," the board said in a news release. "Investigators are pursuing a theory that the massive explosion which led to the destruction of the plant was caused by an ignitable dust cloud," it said.** The state Division of Occupational Safety and Health said the plant was inspected in October, cited for safety violations and fined about \$10,000, which was reduced to about \$9,000 early this month. North Carolina Deputy Labor Commissioner John Johnson said the violations were relatively routine.

Source: http://www.washingtonpost.com/wp-dyn/articles/A5013-2003Jan3_1.html

[\[Return to top\]](#)

Defense Industrial Base Sector

7. *January 31, Inside the Air Force* — **DOD to field data sharing system for homeland defense in 90 days.** The Pentagon plans to field within 90 days a pilot project that will provide a rudimentary information sharing capability across the reaches of the Defense Department, and this system could serve as a multi-agency information-sharing model for the budding Department of Homeland Security, according to a senior Pentagon official. **Project "Protect America," which will largely deal with unclassified information in its early phases, is expected to foster a new mindset of information sharing among and set standards for various Pentagon entities, eventually breaking through the "need-to-know" security walls that can lead to oversights and inefficiencies, according to a separate defense official. DOD's vast experience with information technology and big budget prompted officials on the Joint Chiefs of Staff to take the lead in what is likely to evolve into a government-wide information sharing environment that could link information from the Federal Bureau of Investigation and Transportation Security Administration among others, according to Army Lt. Gen. Joseph Kellogg, Joint Staff director of command, control, communications and computer systems. FBI Director Robert Mueller was briefed on the project and has "shown support for it," according to a separate senior military official. Additionally, top officials in the Transportation Security Administration, the National Guard and the police departments of the 10 largest U.S. cities have expressed interest in participating in the endeavor, the senior official added. Kellogg is expected today to brief Defense Secretary Donald Rumsfeld on the project, according to a DOD official. Homeland Security Secretary Tom Ridge will be briefed on the project in a few weeks, the senior military official said.**

Source: <http://ebird.dtic.mil/Jan2003/s20030131150589.html>

8. *January 31, Washington Post* — **Pentagon plan seeks annual budget boost of \$20 billion.** The Pentagon has prepared a \$399.1 billion defense budget for fiscal 2004 as part of a spending plan that grows by about \$20 billion annually over the next five years and surpasses half a trillion dollars by the end of the decade, according to Defense Department documents. **The plan, which could change slightly between now and President Bush's formal budget submission Monday, calls for a \$16.9 billion increase in the fiscal year that begins Oct. 1, a 4.4 percent increase over the Pentagon's current \$382.2 billion budget.** "We've come full circle," said Steven M. Kosiak, director of budget studies at the Center for Strategic and Budgetary Assessment, a Washington think tank. "We're not only not cutting defense anymore, but we've come to the point where we're spending more money than we spent during the Cold War. Whether this is sustainable over the next six years is questionable." In budget briefings today, aides to Defense Secretary Donald H. Rumsfeld will portray the budget as a blueprint for "transforming" the U.S. military for the information age while maintaining the global war on terrorism and continuing to improve pay and housing for service members, according to a 34-page briefing.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A3417-2003Jan30.html>

9. *January 31, Aerospace Daily* — **Bush gives U.S. STRATCOM four new missions .** President Bush has signed a directive authorizing U.S. Strategic Command (STRATCOM) to assume responsibility for four new missions, according to the command's deputy commander, Air Force Lt. Gen. Thomas B. Goslin, Jr. **The authorization, which had been expected, was signed**

Jan. 10, Goslin said at a conference here. The missions are global strike, integrated missile defense, integrated information operations, and global command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). In the message, an internal memorandum that has not been announced to the public, Bush approved an order giving the missions to U.S. Strategic Command. It said Adm. James O. Ellis, commander of STRATCOM, must give the president, on or before next Jan. 1, an assessment of the command's ability to carry out the missions, and whether extra capabilities are needed to do so. **Goslin, speaking Jan. 29 at "Spacecomm 2003," sponsored by the local chapter of the Armed Forces Communications and Electronics Association (AFCEA), said the action significantly boosts the responsibilities of Strategic Command. The command was established Oct. 1, 2002, but isn't expected to be fully operational for some months.**
Source: <http://ebird.dtic.mil/Jan2003/s20030131150723.html>

[[Return to top](#)]

Banking and Finance Sector

10. *January 30*, — Canada's biggest identity theft?. IBM has lost a hard drive containing the records of 180,000 clients of an insurance company. Details include "names, addresses, beneficiaries, social insurance numbers, pension values, pre-authorized checking information and mothers' maiden names", according to wire reports. Anything else? Oh yes, their bank account details. But is it carelessness, or is it theft? No one knows yet, but the hard drive was stored in a supposedly secure facility in Regina, SK, at ISM Canada, an IBM subsidiary. Local police and the RCMP (the Mounties) are investigating. Meanwhile, Co-operators General Insurance Co. has sent a letter to 180K clients this week, warning them of the possibility of identity theft. And worse could be yet to come: ISM Canada has admitted that the hard drive contains records from other clients. But it won't say who. So let the Toronto Star fill in some of the gaps: The Saskatchewan government has confirmed the missing hard drive contained many crucial files. Workers' Compensation Board records, thousands of public servant pension statements, bulk fuel rebate applications, SaskPower billings, doctor pay lists and physician service data are on the missing hard drive.
Source: <http://www.theregister.co.uk/content/55/29117.html>

11. *January 29, Dow Jones Newswires* — U.S. Customs to open UAE offices to track terrorist money. The U.S. Customs Service is opening offices in the United Arab Emirates – its first permanent base in the Middle East – to help track terrorist financial flows and money-laundering in a country often described as one of al Qaeda's financial hubs. **The service has gained "all approvals" needed to open attache offices in the coming months at the U.S. embassy in the capital, Abu Dhabi, and the U.S. consulate in Dubai, the country's commerce-oriented second emirate, but doesn't have an exact date for the agents' arrivals, U.S. Customs spokesman Dean Boyd told Dow Jones Newswires. The U.S. and UAE have cooperated more closely in tracking terrorists and their money flows since Sept. 11, 2001, when Washington became concerned that the UAE, home to one of the 19 hijackers, had acted as a node for al Qaeda money transfers. In response to Western concern over the emirates' lackluster regulation, the central bank has speeded up legislation controlling money-laundering and has started to regulate hawala, an informal money transfer**

system that has been linked to al Qaeda. **As part of their brief, the UAE-based customs agents will coordinate Operation Green Quest, a multi-agency financial crimes task force led by the Customs Service, which targets the systems used by terrorists to raise and move funds. The agents will also address issues of trade. The Customs Service has representatives in 31 countries across the globe. Its regional operations are currently covered by the attache office in Rome.** The service also plans to open a new office in Switzerland.

Source: http://story.news.yahoo.com/news?tmpl=story/0129/bs_dowjones/200301291000000714

[\[Return to top\]](#)

Transportation Sector

12. *January 31, New York Times* — Citing danger to planes, group seeks ban on a sniper rifle.

A gun-control group has begun a new campaign against large sniper rifles, **asserting that the rifles together with armor-piercing ammunition that bursts into flames on impact pose a serious threat to airliners at airports.** The guns, .50-caliber rifles, sell for thousands of dollars and are primarily purchased by military and law enforcement personnel, but hundreds are bought by civilians every year. **Some manufacturers' marketing material emphasizes that the rifles can destroy aircraft and armored personnel carriers.** The Violence Policy Center produced a 32-page report that it is distributing this week on the potential threat to aircraft of the rifle, which has a range of more than a mile. **The Transportation Security Administration, however, does not see the rifles as a major threat.** Robert Johnson, the agency's chief spokesman, said: "We are aware of it. We have considered it as part of a number of potential threats. We just don't feel it is high on the list of potential dangers." The full text of the report is available at <http://www.vpc.org/graphics/birdhuntingstudy.PDF>

Source: <http://www.nytimes.com/2003/01/31/national/31RIFL.html?ntem ail1>

13. *January 31, Associated Press* — Airlines want federal help in case of war. Airline executives worried about the financial fallout of military action in Iraq want the government to consider easing the burden several ways, including tax relief and a temporary relaxation of antitrust laws. "We need a national transportation plan if we go to war," Continental Airlines' chairman and chief executive, Gordon Bethune, said Thursday at a gathering of tourism and transportation leaders in New York. **In the event of war, major carriers want the right to discuss flight schedules with each other — something prohibited by antitrust law. By coordinating routes and flight frequencies, carriers can reduce service where demand is low without giving up market share.** Executives say it also would ensure that adequate service is maintained in smaller markets, where capacity is most likely be cut first. **Other proposals on the struggling industry's wish list include a temporary suspension of the \$2.50 security tax levied per passenger on each flight, some relief on fuel taxes and the release of oil from the Strategic Petroleum Reserve in order to keep fuel prices down.** U.S. airlines lost billions of dollars in the past two years, despite massive layoffs and reductions in service, and most are not expected to turn a profit in 2003. Executives blame the industry's woes on higher security costs since the September 11 attacks, a significant loss of revenue from business travelers and higher fuel prices.

Source: <http://www.cnn.com/2003/TRAVEL/01/31/airlines.lobbying.ap>

Postal and Shipping Sector

14. *January 30, U.S. Customs Service* — **Enforcement of 24-hour rule begins February 2.** U.S. Customs Commissioner Robert C. Bonner announced that the Customs Service will begin enforcing the 24-hour advance manifest regulation on Sunday, February 2. The 24-hour rule requires sea carriers and NVOCCs (Non-Vessel Operating Common Carriers) to provide U.S. Customs with detailed descriptions of the contents of sea containers bound for the United States 24 hours before the container is loaded on board a vessel. The rule allows U.S. Customs officers to analyze the container content information and identify potential terrorist threats before the U.S.-bound container is loaded at the foreign seaport, not after it arrives in a U.S. port. **Initially, enforcement efforts will focus only on significant violations of the cargo description requirements of the 24-hour rule.** For example, the use of such vague cargo descriptions as "Freight-All-Kinds," "Said-To-Contain," or "General Merchandise," will no longer be tolerated. **Beginning Sunday, Feb. 2, 2003, U.S. Customs Service ports will issue "Do-Not-Load" messages to sea carriers and NVOCCs that violate the 24-hour rule. The "Do-Not Load" message instructs these parties not to load a specific container that has been found in violation of the 24-hour rule. Carriers and NVOCCs that disregard these "Do Not Load" messages (and load the cited container) will be denied permission to unload this container at any U.S. port.** Customs has posted a "Frequently Asked Questions" (FAQs) section on its Web site (www.customs.gov) to assist carriers, NVOCCs and others in understanding the expectations of the U.S. Customs Service concerning the 24-hour rule. Source: http://www.customs.gov/xp/cgov/newsroom/press_releases/01302_003.xml

Agriculture Sector

15. *January 31, Wisconsin Ag Connection* — **Beef producers fear new rule would be costly.** U.S. cattle producers may be facing some expensive and complicated record-keeping procedures if they are to comply with a new country-of-origin food labeling law that will become mandatory next year. The law will apply to many foods and for beef it will soon require that each package have a label listing where the cattle were born, raised, and slaughtered. Also, supermarkets and beef plants must have documentation supporting those labels. Failure to supply such documentation can result in fines up to \$10,000, according to officials. "We are faced with a problem we do not know how to deal with," said Richard McDonald, president and chief executive officer of the Texas Cattle Feeders Association, who said his organization has not yet developed a compliance plan. The country-of-origin labeling law is part of the 2002 Farm Bill. Beginning in September 2004 supermarket packages of beef, veal, lamb, pork, fish, fruits and vegetables, and peanuts must contain country-of-origin labels. Source: <http://www.wisconsinagconnection.com/story-national.cfm?Id=132t>

16. *January 31, Denver Post* — **Eased cattle-grazing rules sought.** The Bush administration on

Thursday proposed rolling back several Clinton-era restrictions on cattle grazing. Bureau of Land Management (BLM) Director Kathleen Clarke announced the proposed changes in a speech to the Centennial-based National Cattlemen's Beef Association meeting in Nashville. **Her proposals would: allow ranchers to hold property interests in the fences, stock ponds, and equipment they put on publicly owned land, require the BLM to take the local culture and economy into account when doing environmental studies of grazing on federal land, streamline the appeals process for grazing decisions, and extend to five years the amount of time a grazing allotment can go ungrazed before a rancher loses it under so-called "use it or lose it" rules.**

Source: <http://www.denverpost.com/Stories/0,1413,36%257E53%257E1147835%257E.00.html>

[\[Return to top\]](#)

Food Sector

17. *January 31, Reuters* — UN health agency issues alert on food terrorism. The World Health Organization (WHO) warned on Friday that terrorists could try to contaminate food with chemical, biological, or radioactive agents and urged states to tighten their defenses. It said such an attack could result in people dying, being paralyzed, or contracting illnesses such as cancer. The UN agency called on its 192 member governments and on industry to boost surveillance and emergency response measures to minimize the risk. According to the Geneva-based agency, some 1.5 million people, mainly children, already die each year due to diarrhea-related diseases caught from eating contaminated food. There were only relatively few known cases of deliberate contamination, but they should serve as a warning, it said. **"Threats from terrorists, criminals, and other anti-social groups who target the safety of the food supply are already a reality,"** WHO said, adding it had received no specific threats of any such attack. **"Deliberate release of a chemical, biological, or radionuclear agent could potentially cause severe harm and pose a huge burden on public health systems,"** it added. Biological agents are pathogens including viruses, bacteria, and parasites, while deadly chemical agents can range from pesticides to cyanide. Radionuclear agents include uranium. Source: <http://www.alertnet.org/thenews/newsdesk/L31218635>

18. *January 30, Center for Infectious Disease Research and Policy* — FDA proposes rules for advance notice of food imports. Starting next December, importers will have to start notifying the Food and Drug Administration (FDA) at least a day in advance of every food shipment coming into the United States. That requirement is likely to generate an average of about 20,000 shipment notices daily, the FDA said in announcing proposed regulations to implement it. **The requirement is part of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. The requirement will "allow FDA to target inspections more effectively and to help ensure the safety of imported food products before they enter domestic commerce,"** the agency said in a news release yesterday. "The more we know about the source of the food we eat the better prepared we'll be to monitor its safety," Secretary of Health and Human Services (HHS) Tommy Thompson said in the news release. **The FDA also proposed rules for implementing a requirement that food manufacturing and processing facilities register with the agency. That requirement is also part of the 2002 bioterrorism law and will take effect Dec 12 of this year.** Farms,

restaurants, retail food stores, nonprofit food services, and facilities (such as slaughterhouses) that are regulated exclusively by the U.S. Department of Agriculture (USDA) are exempt from the requirement. Regarding food imports, the FDA proposes to require notification by noon of the day before the food will arrive at the border crossing or port of entry. **The new law says that "food imported or offered for import without adequate prior notice will be refused admission and held at the port of entry until adequate prior notice is received, unless FDA directs its removal to a secure facility," the FDA said.**

Source: <http://www1.umn.edu/cidrap/content/biosecurity/food-biosec/news/foodship.html>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

19. *January 31, CNN* — **Georgia blood supply being held for quality review. Hospitals in Georgia are being asked to hold some units of donated blood and are making blood available only for emergency use, the Red Cross said Friday.** The Red Cross is "being overly cautious and erring on the side of safety" by holding some of the blood supply for quality review, said Candice Gouldin, director of communications for Red Cross' Blood Services Southern Region, which is responsible for all donor blood supplies in the state of Georgia and some of Florida. **Kevin Bloy, spokesman for the Georgia Hospital Association, said all of the group's members have been notified to hold blood while the Red Cross investigates a problem with blood bags.** Bloy added that a significant amount of surgeries will be affected in Georgia, especially those that require large amounts of blood.

Source: <http://www.cnn.com/2003/HEALTH/01/31/georgia.blood/>

20. *January 31, Los Angeles Times* — **Big cuts planned in health care. Cuts proposed to help balance Orange County, California's budget would limit health care for the poor, could put more mentally ill patients on the street, and slow authorities' response to outbreaks of disease.** Cutbacks in the county laboratory also would affect the timeliness of water testing, potentially exposing swimmers and surfers to disease-causing bacteria, according to a list of \$8.4 million in programs and services identified Wednesday to help trim the county's \$4 billion budget. If the cuts are enacted, it is likely that some of the smaller county-run clinics would close, said Pat Markley, a spokeswoman for the Orange County Health Care Agency. The clinics provide free immunizations, testing for and treatment of tuberculosis, venereal disease, and prenatal care. **Officials said the shortfall is the result of the county being caught in the squeeze of the state budget crisis, which could mean tens of millions less for Orange County.** It also must grapple with reduced revenue from property taxes as well as the huge debt incurred during the 1994 bankruptcy. **The proposed \$8.4 million in cuts for the fiscal year beginning July 1 would amount to about 11% of the \$71 million the health agency gets from the county. An additional \$2.5 million in cuts is recommended the next year.**

Source: <http://www.latimes.com/news/local/orange/la-me-cuts31jan31.0>

21. *January 30, Associated Press* — **Bill would require meningitis vaccine. College students would be required to take meningitis vaccines under a bill proposed Thursday in the Georgia House.** The bill was introduced a week after a Georgia Southern University student was hospitalized for bacterial meningitis, an infection of spinal cord fluid and the fluid surrounding the brain that can be caused by bacteria or by a virus. GSU started offering \$90 vaccines to students Thursday. The proposed bill would require college students to pay for the vaccines themselves, just as they are currently responsible for getting shots against measles, mumps and rubella before enrolling. Doctors say college students are at special risk for contagious diseases because they live in close quarters.

Source: http://augustachronicle.com/stories/013103/met_124-1486.shtm1

[[Return to top](#)]

Government Sector

22. *February 02, Washington Post* — **Homeland Security office to take part in shuttle disaster investigation.** Government officials quickly concluded on Saturday that terrorism or other foul play were not the likely causes of the breakup of the space shuttle Columbia over Texas, though they cautioned that they will investigate all possibilities. **Within an hour of the disaster, Tom Ridge, secretary of the new Department of Homeland Security which is responsible for evaluating all major domestic incidents, was conferring with intelligence analysts and national security officials at the White House.** "They were able to determine fairly early on that we didn't have information or indicators of terrorism at this time," said Homeland Security Department spokesman Gordon Johndroe. Within minutes of the aircraft's disappearance, military authorities from the Pentagon's national command center and from Strategic Command in Omaha and Northern Command in Colorado joined a conference call with leaders of federal civilian agencies to discuss how to respond. **Known as a domestic event conference, the phone link stayed open throughout much of the day as emergency actions took shape.** One administration official said authorities had learned of a threat against the Columbia associated with a previously scheduled July 19 launch date, but the information was determined "not credible." There were no threats made against the Columbia since then, he said. **"The only threats associated with the shuttle were from many, many months ago,"** the official said. He noted that the shuttle broke up too far from Earth to have been fired upon by surface-to-air missiles. Security for the mission was especially tight because of the presence of an Israeli astronaut, Ilan Ramon. **Ridge put the Federal Emergency Management Agency in charge of recovering debris from the shuttle, and Defense Secretary Donald H. Rumsfeld assigned Northern Command responsibility for military forces assisting in the search.** Initiated after the Sept. 11, 2001, attacks, the command was established in October to coordinate the use of federal forces in domestic emergencies.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A12959-2003Feb 1.html>

23. *February 02, New York Times* — **INS extends start date for system tracking foreign students.** Backlogged in its efforts to give colleges approval to use a new electronic tracking system for foreign students, the Immigration and Naturalization Service (INS) has **announced**

a two-week extension of the deadline for institutions to begin using the system. The \$36 million Student and Exchange Visitor System, or Sevis, was to become the sole mechanism for schools to transmit information about the identities, addresses and academic standing of nearly one million foreign students and scholars on their campuses by midnight Thursday. **While the immigration service has given approval to 3,400 high schools, colleges, universities and trade schools to use Sevis, more than 2,000 are still awaiting permission, said Christopher Bentley, an agency spokesman. Without it, the institutions may not accept new foreign students.** Moreover, as the immigration service has allowed more and more institutions to log on, complaints that the system appeared slow and overloaded have grown.

Source: <http://www.nytimes.com/2003/02/02/politics/02VISA.html>

24. *January 30, Washington Post* — **Ridge outlines new border security plans.** President Bush will ask Congress to devote \$41.3 billion to homeland security in the 2004 federal budget, Tom Ridge, the secretary of the new department, said Thursday. **That figure represents an increase over the \$37.7 billion spent last year on homeland security across the government, including the military. Ridge announced the budget increase in Miami, where he paid his first public visit to department employees since his confirmation last week.** On Thursday alone, Ridge said, workers would deal with more than 1 million people crossing U.S. borders, process 2.4 million pieces of luggage at airports and inspect tons of imported food products – not to mention handle thousands of visa and green card applications. "The sheer depth and breadth of this nation, the magnitude of what occurs here from sea to shining sea, means simply that one slip, one gap, one vengeful person can threaten the lives of our citizens at any time, in any number of ways," Ridge said. "We will organize to mobilize. It will lead to outcomes that better protect our country." **Under the president's proposal, the Homeland Security Department alone would have a budget of \$36.2 billion in the fiscal year that begins in October. That is just short of a 10 percent increase above the combined budgets of all the agencies being rolled into it. A good deal of the new spending is devoted to upgrading Coast Guard ships and aircraft, agency officials said.** Ridge described plans to combine border security and inspection agencies to streamline the entry process and increase the chance of catching terrorists and weapons at the border. People entering the United States would ideally meet with a single Homeland Security officer who would oversee all matters of customs, immigration and law enforcement, he said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A3543-2003Jan3 0.html>

[\[Return to top\]](#)

Emergency Services Sector

25. *February 02, Washington Post* — **Rain of metal rattles those on the ground.** The space shuttle Columbia cascaded to Earth Saturday morning in a furious shower of shrapnel from a crystalline blue sky, spreading over hundreds of square miles from northern Texas to Louisiana. **A deafening roar punctuated by terrible booms startled people from their beds. Windows, roofs and tiles trembled. Suburban dogs barked madly at the heavens. There was a staccato pop-pop-pop of unknown objects hurtling to the ground like deadly hail. Miraculously, perhaps, no one on the ground was seriously hurt. But many were seriously frightened.** Authorities in Hemphill, Tex., near the Louisiana border, said human remains from the shuttle had been found in woods and open fields there. Sgt. Daniel Young of the Texas

Rangers said four parts of human bodies, including some limbs, had been collected by federal officials and taken to a morgue. A helmet and clothing also were found. **The detritus of the shuttle rained down from Dallas to the southeast, setting small fires, leaving fields and forests smoldering. One hefty slab also slammed into the grassy median strip of a four-lane road north of the East Texas town of Palestine.** A barrel-shaped chunk fell like a bomb on the Nacogdoches airport's landing strip. In and around the town, neighborhoods were littered with the debris of Columbia. That was just what people saw. No one knew how much had fallen in the dense piney woods of East Texas, outside the towns and off the main roads. Some guessed that souvenir hunters could be finding pieces for years. **"We've found pieces from the size of a dime up to 6 feet by 6 feet," said Larry Hobson, 45, fire chief of the town of Douglass, 15 miles west of Nacogdoches.** As radio and television reports amplified warnings from NASA and other authorities not to touch any of the debris, people trickled into the emergency room at Nacogdoches Memorial starting around 10 a.m. — some of them carrying the pieces they had found. "Some of the folks brought the pieces of the debris with them to the hospital. Pieces of this thing are all over the place," said G.W. Jones, assistant administrator of the county hospital. Security guards screened people outside the hospital before the debris was brought inside. One of the pieces was about the size of a hand, he said; all of it was being turned over to the National Guard. **Jones said 27 people had turned up at the emergency room seeking information about possible side-effects from contact with Columbia's flotsam. But despite the dire warnings from officials, there were no apparent injuries — "not even an abrasion from this thing," he said. "They are very calm. They just kind of need to know what they should do in case they have any side-effects developing at some later point."**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A12536-2003Feb.1.html>

26. *February 01, Federal Emergency Management Agency* — **FEMA to lead search, find, and secure mission following space shuttle tragedy.** The Federal Emergency Management Agency (FEMA) has been designated as the lead federal agency for the search, find, and secure efforts in response to the loss of space shuttle Columbia. Michael Brown, Deputy Director of FEMA and Acting Undersecretary of Homeland Security for Emergency Preparedness and Response, will lead FEMA's efforts. **"FEMA has been asked to lead the federal effort to search, find, and secure debris from Columbia so that NASA can move forward with a full investigation. We are working closely with several federal agencies as well as state and local officials in Texas and Louisiana to make sure that all available resources are coordinated and used effectively in this important mission."** Brown has been in contact with Secretary of Homeland Security Tom Ridge, NASA Administrator Sean O'Keefe and U.S. Defense Department officials throughout the day, and is working through the emergency management offices of Texas and Louisiana to determine what response assets have already been deployed and which additional assets might be available for the mission.

Source: http://www.fema.gov/nwz03/nwz03_027.shtm

27. *January 31, New York Times* — **State Department link will open visa database to police officers.** Law enforcement officials across the country will soon have access to a database of 50 million overseas applications for United States visas, including the photographs of 20 million applicants. **The database, which will become one of the largest offering images to local law enforcement, is maintained by the State Department and typically provides personal information like the applicant's home address, date of birth and passport number, and**

the names of relatives. It is a central feature of a computer system linkup, scheduled within the next month, that will tie together the department, intelligence agencies, the FBI and police departments. The new system will provide 100,000 investigators one source for what the government designates "sensitive but unclassified" information. Officials see it as a breakthrough for law enforcement, saying it will help dismantle the investigative stumbling blocks that were roundly criticized after the Sept. 11 attacks. At the same time, they acknowledge the legal and policy questions raised by information sharing between intelligence agencies and local law enforcement, and critics have cast a wary eye as well at the visa database. **One other effect of the new system is that for the first time, the Federal Bureau of Investigation and other agencies linked by it will be able to send one another encrypted e-mail. Previously, security concerns about the open Internet often caused sensitive information to be faxed, mailed or sent by courier.**

Source: <http://www.nytimes.com/2003/01/31/national/31COMP.html>

[\[Return to top\]](#)

Information and Telecommunications Sector

28. *February 02, New York Times* — **Departing security official highlights cyber threat.** Richard A. Clarke, the blunt, sometimes abrasive White House adviser who raised the alarm about unconventional national security threats ranging from failed states to biological and computer terrorism for more than a decade, quietly resigned as President Bush's special adviser for cyberspace security on Friday. **In an interview after his last day in office, Clarke warned that although the government had made considerable progress in defending its electronic infrastructure from computer attacks, the United States faced ever greater peril, given its growing dependence on the Internet. "A sophisticated cyberattack may not result in massive deaths," he said. "But it could really hurt our economy and diminish our ability to respond to a crisis, especially if it is combined with a war, or a terrorist attack."** Clarke said the attack last weekend by a computer bug known as the Sapphire worm showed the vulnerability of the United States' increasingly Internet-based economy. Though it was a relatively simple bug, he said, Sapphire, which has also been called Slammer, ravaged systems throughout the United States and overseas in just a few hours, shutting down some of the Bank of America's automated teller machines and Continental Airlines' online ticketing system, and denying access to the Internet to millions of personal computer owners. "Don't assume that the damage done by hackers in the past is predictive of the future," Clarke said. "As Sept. 11 showed, as long as our vulnerabilities are large, some enemy will exploit them in a new and hugely damaging way." **Clarke said the nation is safer today than before Sept. 11 because al Qaeda's sanctuary in Afghanistan is gone and because Americans had rounded up hundreds of al Qaeda operatives abroad and tightened aviation security overseas and domestically. Clarke said he was leaving his post now because "11 years in the White House and a total of 30 in government is more than enough," and because President Bush would soon unveil a new national strategy to protect the nation's information infrastructure, which Clarke and his team had drafted.**

Source: <http://www.nytimes.com/2003/02/02/politics/02RESI.html>

29. *January 31, Federal Computer Week* — **Cybersecurity RDagenda unveiled.** The Institute for Information Infrastructure Protection (I3P) has unveiled its 2003 Cyber Security

Research and Development Agenda, which identifies critical areas that require significant research and development to help secure the nation's information infrastructure. The agenda, announced January 30, outlines eight crucial RDgaps that are not being sufficiently addressed by ongoing government, private-sector or academic research: 1) Enterprise security management; 2) Trust among distributed autonomous parties; 3) Discovery and analysis of security properties and vulnerabilities; 4) Secure system and network response and recovery; 5) Traceback, identification and forensics; 6) Wireless security; 7) Metrics and models; 8) Law, policy and economics. The I3P, a consortium of 23 leading cybersecurity research institutions from academia, national labs and nonprofit organizations, is funded by the Commerce Department and the National Institute of Standards and Technology. **The agenda will help the White House's Office of Science and Technology Policy better coordinate RDefforts across government agencies,** said Susan Hays, deputy associate director for technology at the office. I3P received input, gathered over nine months in 2002, from more than 900 experts and security professionals from the private sector, academia and government, said Michael Vatis, chairman of I3P.

Source: <http://www.fcw.com/fcw/articles/2003/0127/web-cyber-01-31-03.asp>

30. *January 31, Computerworld* — **Free benchmark could have found Slammer vulnerability.** Industry experts and users said the Slammer worm should have been a non-issue for companies because **the patches and a free tool capable of detecting the vulnerability exploited by the worm were available six months ago.** In particular, they point to the issuance in July of the Consensus Minimum Security Benchmarks, also known as the Gold Standard. Developed jointly by five federal agencies, including the National Security Agency (NSA) and the FBI's National Infrastructure Protection Center, as well as the SANS Institute and the Center for Internet Security (CIS), **the Gold Standard benchmark can be used to test Windows 2000 Professional systems running as workstations for proper configuration.** Alan Paller, director of research at SANS, said an NSA study of the benchmark concluded that **by running it on a network a company could eliminate more than 90% of known vulnerabilities.** Claude Bailey, an IT security analyst at one of the nation's largest financial management firms, said that while the Gold Standard is a good starting point, his security administrators say **the problem isn't in detecting the vulnerability but in deploying the patches and fixes across an organization of 50,000 employees -- and guaranteeing that the patch won't cause more problems.** "We tested the original patch [for the SQL vulnerability], and it had problems," said Bailey. Now, with the financial firm in the middle of tax season, there's too much to lose to deploy patches that break other parts of the network.

Source: <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,78063,00.html>

31. *January 30, SecurityFocus* — **E-voting security debate. Some respected computer scientists and security experts in California's Silicon Valley say the risks posed by malicious hackers, equipment failure or subtle programming errors make fully-electronic voting systems a bad idea.** "There's no voter-validated record, so Trojan horses or accidents can happen without any evidence that anything has gone wrong," correctly," says Peter Neumann, a scientist at SRI International, a non-profit research institute. Electronic voting systems usually featuring touch screens and simple ATM-like interfaces. By some estimates one out of five votes were cast electronically last November. **The systems are not connected to the Internet; instead, voters' ballots are typically stored on an internal hard drive until the polls close.**

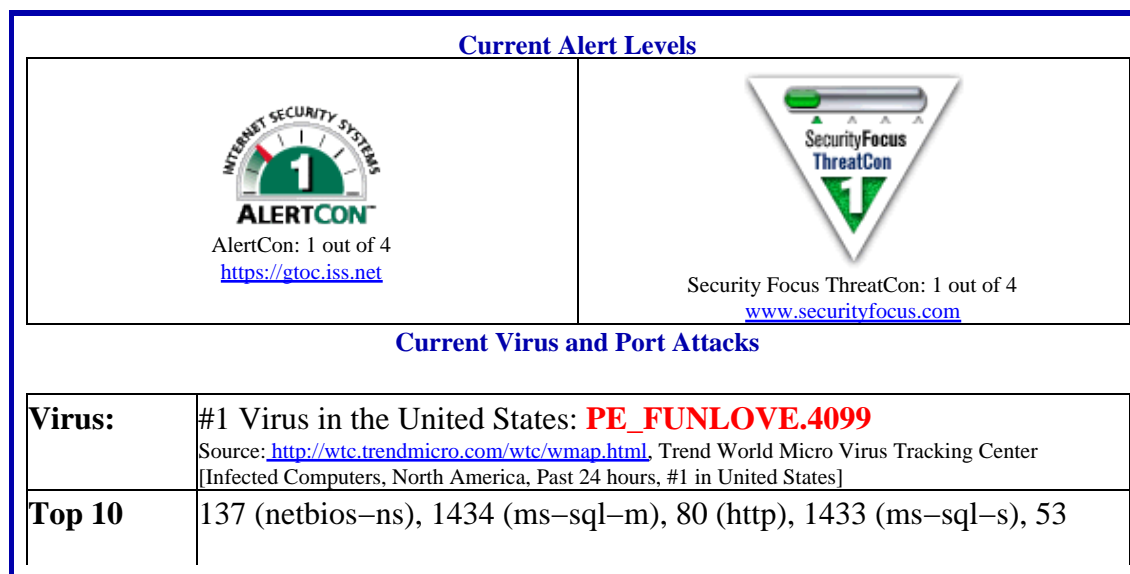
Then they're copied a portable disk or a non-volatile memory card and taken to a central counting facility. It's the paperless nature of the transaction that bothers critics. "The problem is that...it's really up to the company that wrote the software to say that there were no errors or deliberate tampering that interfered with the vote," says David Dill, a computer science professor at Stanford University. The computer scientists say they'd be happier, but not convinced, if companies making the electronic voting systems released their code for public review. On Friday they are going to attempt to persuade Santa Clara County to embrace a system in which electronic voting stations print a hard copy of the voter's ballot. The voter can then review the printout before manually depositing it in a ballot box.

Source: <http://online.securityfocus.com/news/2197>

32. *January 29, Silicon.com* — Exposed server is a magnet for hack attacks. The amount of hacking activity on the Internet has been revealed after one company set up an anonymous 'dummy test' server—and found it was maliciously attacked 467 times within 24 hours of being installed. The server, which contained no data and had no public profile, was attacked every single day over the next three weeks. PSINet Europe ran the test on an unprotected server at its Internet Data Center in Amsterdam, and registered a total of 626 malicious attacks over the three week period. A significant number of attacks originated from broadband or cable ISPs. PSINet's report into the experiment says that: "High bandwidth links do not only provide end users with faster download times—they also allow hackers to attack a wider target audience with a wider array of tools." PSINet also found that the bulk of the attacks originated from the United States and Western Europe and not in the most commonly expected areas of the former Eastern Bloc countries. Within Europe, Germany, Italy, the Netherlands and the UK were the most popular locations, while the countries most associated with attackers—Russia, Bulgaria and Romania—did not even feature. The findings of the PSINet Europe test are backed up by figures from the Gartner Group, which reported that 90 per cent of security breaches occur as a result of networks being incorrectly configured and managed.

Source: <http://zdnet.com.com/2100-1105-982554.html>

Internet Alert Dashboard



Target Ports	(domain), 21 (ftp), 139 (netbios-ssn), 445 (microsoft-ds), 135 (???), 4662 (???) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
---------------------	---

[[Return to top](#)]

General Sector

33. *January 30, Associated Press* — Report: Al Qaeda made bomb in Afganistan. British officials believe that Osama bin Laden's al Qaeda terrorist network successfully built a crude radiological device known as a "dirty bomb" in Afghanistan, the British Broadcasting Corp. reported Thursday. **British intelligence agents found documents that showed al Qaeda members had built a small device near Herat in western Afghanistan, the BBC said, citing unidentified British government officials.** Britain's Foreign Office said Thursday the report substantiated expert opinion that al-Qaida wanted to develop a nuclear weapon. "The evidence presented in the BBC report speaks for itself," a spokesman told The Associated Press. "It provides proof to substantiate expert opinion that al-Qaida was interested in developing nuclear weapons." In Washington, a U.S. official, speaking on condition of anonymity, said bin Laden was no doubt interested in acquiring a "dirty bomb" — a conventional bomb capable of spreading radiation. **But the U.S. official said, "We have no evidence to substantiate that he's built such a device."** The British intelligence agents did not find the device itself and it has not since been recovered, BBC reported. **But scientists at the British government's weapons research facility in Porton Down concluded that al Qaeda had succeeded in constructing a small "dirty bomb" in Herat — based on documents and material uncovered by the British military and intelligence, the BBC said.** The scientists did not believe al Qaeda had been able to develop a full-blown nuclear device, it said. The report did not say when the device was thought to have been developed or how much radiation it could spread.

Source: http://story.news.yahoo.com/news?tmpl=story_p_on_re_eu/britain_dirty_bomb_1

[[Return to top](#)]

NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

NIPC Advisories – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

NIPC Alerts – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

[NIPC Information Bulletins](#) – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

[NIPC CyberNotes](#) – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure–related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:	Melissa Conaty (202–324–0354 or mconaty@fbi.gov) Kerry J. Butterfield (202–324–1131 or kbutterf@mitre.org)
Distribution Information	NIPC Watch and Warning Unit (202–323–3204 or nipc.watch@fbi.gov)

NIPC Disclaimer

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.